Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Méréstechnika és Információs Rendszerek Tanszék

Vasúti fékrendszer modellezése és megbízhatósági vizsgálata

Szakdolgozat

Készítette
Ábrahám Dániel

Konzulens
dr. Vörös András
Suszter Máté

2021. december 19.

Tartalomjegyzék

HALLGATÓI NYILATKOZAT

Alulírott *Ábrahám Dániel*, szigorló hallgató kijelentem, hogy ezt a szakdolgozatot meg nem engedett segítség nélkül, saját magam készítettem, csak a megadott forrásokat (szakirodalom, eszközök stb.) használtam fel. Minden olyan részt, melyet szó szerint, vagy azonos értelemben, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Hozzájárulok, hogy a jelen munkám alapadatait (szerző(k), cím, angol és magyar nyelvű tartalmi kivonat, készítés éve, konzulens(ek) neve) a BME VIK nyilvánosan hozzáférhető elektronikus formában, a munka teljes szövegét pedig az egyetem belső hálózatán keresztül (vagy autentikált felhasználók számára) közzétegye. Kijelentem, hogy a benyújtott munka és annak elektronikus verziója megegyezik. Dékáni engedéllyel titkosított diplomatervek esetén a dolgozat szövege csak 3 év eltelte után válik hozzáférhetővé.

Budapest, 2021. december 19.

Ábrahám Dániel
hallgató

Kivonat

Modern világunkban elengedhetetlen a biztonságos és megbízható utazás. Egyre összetettebb közlekedési rendszereknél létfontosságú lépést tartani a növekedett komplexitás melletti gyors fejlesztés és főleg a fejlesztés biztonságosságának bizonyítása. Manapság elképzelhetetlen lenne szabványok nélkül kritikus rendszert fejleszteni. Nincs ez másképp a vasútiparban sem.

A vasúti fékrendszer az egyik legkritikusabb eleme a biztonságos közlegedésnek, főleg a városi közlekedésben aktívan résztvevő villamosoknál. Ebben a dolgozatban szeretném bemutatni a modell-alapú rendszertervezés megközelítését, annak előnyeit egy esettanulmány keretében készített valóságszerű vasúti férendszeren keresztül. Az elkészített rendszerterv alapján szeretnék rávilágítani a funkcionális biztonság fontosságára. A diplomamunka célja feltárni az irodalomban fellelhető biztonsági analízis módszereit. Feltárni Top-down és Bottom-up módszereket egyaránt az analízis lehető legszélesebb palettájának elvégzése érdekében. Ezek bemutatása, majd az alkalmasnak választott módszerek részletes bemutatása az esettanulmány során tervezett rendszer alapján.

Abstract

Safe and reliable travel is essential in out modern world. In Transportation systems, getting more and more complex it is vital that one can keep up development time and especially safety with the humongous complexity. Safety-critical development is unimaginable without standards nowadays. Railway systems are no different either.

Railways brake systems are one of the most critical parts of a train, predominantly in tramways that are an active participant of city commute. In this study, I would like to show some of the benefits of model-based systems engineering in a case study about an imaginary railways brake system based on reality. I would like to highlight the importance of function safety with the designed system. Goal of this study is to explore various methodologies for functional safety. Explore a wide palette of methods, Top-down and Bottom-up as well to make a comprehensive range of safety analysis. Showcase their possibilities, and then select a variety of methods to discover their usecases on the designed system during the case study.

1. fejezet

Bevezetés

1.1. Motiváció

Mai világunk elképzelhetetlen lenne hatékony és gyors közlekedés nélkül. Ez főleg érvényes a tömegközlekedési eszközökre, legyen az repülőgép, vonat, metró, villamos vagy más egyéb tömegközlekedési eszköz. Nélkülük szinte képtelenség lenne a nagyvárosi lét.

Napjainkban szinte az élet minden terén egyre komplexebb és komplexebb rendszereket fejlesztenek ki. Így van ez a közlekedési szektor minden részén, benne a vasútiparban is. Emellett a megnövekedett bonyolultság mellett kell lehető leggyorsabban kifejleszteni az adott rendszereket ügyelve a növekedő biztonsági elvárásokra.

A biztonság, rendelkezésre állás és költséghatékonyság problémája jellemzi leginkább a mai globális vasútipart és a vasút környezetét. Ezért a kereslet azokért a rendszerek, amelyek képesek magasfokú biztonságot, rendelkezésreállást és költséghatékonyságot tudnak nyújtani növekedni fog. Különösen igaz ez a vasúti fékrendszerekre.

A növekedő komplexitás és biztonsági követelmények miatt egyre inkább nehézkessé válik a hagyományos dokumentum-alapú fejlesztési módszertan. Ezért dolgozatomban szeretnék bemutatni a vasúti fékrendszeren keresztül egy modell-alapú rendszerfejlesztési megközelítést, bemutatva annak pozitív hatását a komplexitás kezelése érdekében. Továbbá a dolgozat második felében a modellezett rendszer egy vezérlő egységének biztonsági vizsgálatával folytatom.

1.2. A dolgozat felépítése

A dolgozat 2. fejezetében ismertetem a modell-alapú rendszerfejlesztés methodikáját és kis betekintést nyújtok a SysML nyelvbe. A 3. fejezetben irodalmi kutatást végzek a biztonsági analízis módszertanához. A 4. fejezet írja le az esettanulmány hátterét, míg a 5. fejezet az esettanulmány során elkészített vasúti fékrendszer modelljét tartalmazza. A 6. fejezet tartalmazza az esettanulmány során végrehajtott biztonsági vizsgálatot.

2. fejezet

Háttérismeret

2.1. Modellezés

2.1.1. Modell-alapú rendszerfejlesztés

A modell-alapú rendszerfejsztés, angolul rövidítve MBSE[1], egy formalizált módszertan, amely a követelméynkezelés, tervezés, analízis, verifikáció és validáció témaköreiben nyújt segítséget az összetett rendszerek fejlesztése során. A dokumentum-alapú fejlesztéssel ellentétben az MBSE modelleket helyez a fejlesztés középpontjába. A 2020-as évben a NASA[2] is megjegyezte, hogy „A modell-alapú rendszertervezést mind az ipari mind a kormányzati egyre inkább felkarolja, hogy lépést tudjon tartani a rendszer komplexitásával."[1] Az MBSE három különböző koncepciót hoz össze: modell, rendszergondolkodás, rendszerfejlesztés (Shevchenko, 2020 [22])

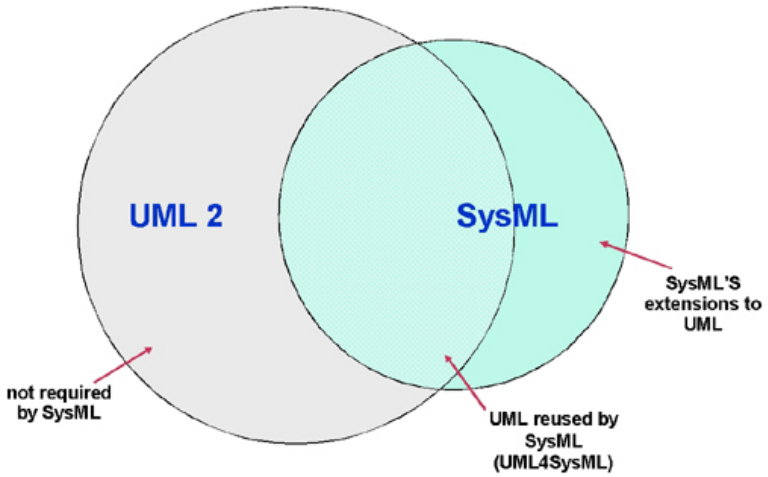
A modell-alapú rendszerfejlesztés növelheti az a teljes termék specifikációhoz tartozó információ megragadásának, vizsgálatának, megosztásának és koordinálásának képességét, amely a következő előnyökkel járhat (Friedenthal, 2007 [10]):

- Javítja a kommunikációt a fejlesztésben részvevők között (például: a vevő, a projekt vezető, a rendszermérnökök, hardver és szoftver fejlesztők, tesztelők stb.).
- Az összetettség menedzselésének javítása.
- Megnövekedett termék minőség.
- A rendszertervezés alapjainak tanítási és tanulási képességének javulása.

Manapság a modell-alapú rendszertervezés számos iparágban jelen van, például: Járműipar, közlekedés, űripar, orvosi eszközök, robotika, nukleáris technológia, ipari rendszrek, gyártás stb. Leginkább olyan környezetekben használatos, ahol valóság korlátos (beavatkozás behatárolt, méret kényszer stb.), fontos az együttműködés több szakmán/beszállítókon keresztül, drága a prototípus gyártás vagy biztonságkritikus rendszereknél (Molnár, 2019 [25]).

[1] Model-based systems engineering

[2] National Aeronautics and Space Administration, Amerikai Egyesült Államok kormányzati ügynöksége



2.1. ábra. A SysML és az UML kapcsolata (Forrás: [16])

2.1.2. SysML

A SysML[3] egy általános célú architektúra modellező nyelv rendszermérnöki felhasználásra. A nyelv támogja számos rendszerek, rendszerek rendszereinek (Systems of systems) specifikálását, vizsgálatát, tervezését, verifikációját és validációját. Ezek tartalmazhatnak hardver/szoftver elemeket, információkat, folyamatokat, személyzetet és létesítményeket. A SysML az UML[4] 2-nek egy dialektusa és egy UML 2 Profilként van definiálva [23].

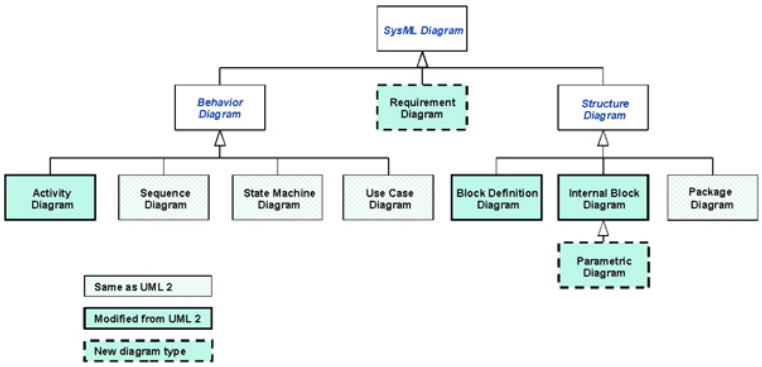
A SysML Cris Kobryn által szervezett rendszermérnökökből és modellező eszköz szakértőkből álló informális szövettség úgy nevezett „SysML Partnekek" által lett létrehozva 2003-ban. Az első kiadás 2005-ben jelent meg és az elsődleges közreműködök között ott volt a Motorola, a Telelogic és a Northrop Grumman is. Másfél évvel az első megjelenés után, 2006-ban hivatalosan is adaptálásra került a specifikáció az OMG[5] által, ezáltal a specifikáció hivatalos neve: OMG SysML 1.0. A mai napig nem történt nagy változás a szabványban. A jelenleg használt legfrissebb verzió az 1.5-ös, bár az OMG 2017-ben benyújtott egy változtatást OMG SysML 2.0 néven [24].

2.1.2.1. Modell elemek

Mint az már fentebb említve lett, a SysML kiegészíti az UML 2 nyelvet. A két nyelv kapcsolatát az 2.1. ábra szemlélteti. Látható, hogy egyes elemek teljesen kikerültek a SysML eszközkészletéből, de számos újdonság került bele.

A SysML struktúrájának alapvető egysége a blokk, amit bármilyen rendszer elem reprezentálására lehet használni (például: hardver, szoftver, létesítmény, személyzet stb.). A rendszerstruktúrát blokk definíciós diagrammok (BDD[6]) és „internal block" diagrammok (IBD[7]) alkotják. A BDD írja le a rendszer hierarhiáját, míg az IDB a belső struktúrát.

[3]Systems Modeling Language
[4]Unified Modeling Language
[5]Object Management Group
[6]Block Definition Diagram
[7]internal block diagram



2.2. ábra. SysML diagramm típusok (Forrás: [16])

A nyelv támogat számos viselkedésleíró diagrammot is. Ezek nagyrésze egyezik az UML-ben definiált párjával. Az egyetlen kivétel az Aktivitás diagramm, amely kissé módosult az adaptáció során.

A hasonlóságokat és különbségeket legjobban az 2.2. ábra mutatja be.

3. fejezet

Irodalmi kutatás

3.1. FIT Allokáció

Az ipari rendszerek egyre összetettebbekké váltak az évek során. Emellett mostanság egyre több ilyen rendszer tartalmaz elektronikát és szoftvert, tehát a funkcionális biztonságnak folyamatosan nő a fontossága.[21]

A RAMS[1] követelmények allokációja szerves részét képezi az alacsonyabb szinten lévő alrendszerek tervezésének rendszer mérnöki folyamatoban. A allokáció célja, hogy megtalálja a leghatékonyabb fizikai architektúrát, ami megfelel a rendszerszintű követelményeknek és az allokáció funkcionális viselkedés analizálása által szervezett. Amikor RAMS konstukció szükséges minden teljesítménybeli követelményfajtára - megbízhatóság, elérhetőség, karbantarthatóság, biztonságosság - külön kell az allokációs folyamatot végezni. Az allokációs módszerek a négy különböző karakterisztikára hasonlók. [4]

Amikor az allokáció a tervezés olyan korai fázisában kezdődik, amikor még nincs elegendő rendelkezésre álló információ az allokációt folyamatosan frissíteni kell a funkcionális analízis során. A rendszer alacsonyabb szintjein lévő allokáció szükséges a termék meghatározási fázishoz és céljaihoz [3]:

- Hogy igazolja a teljes rendszer RAMS követelményeinek megvalósíthatóságát,
- Hogy meghatározzon ellenőrizhető RAMS design követelményeket alacsony szinten és
- Hogy meghatározzon egyértelmű és megvalósítható RAMS követelményeket az alrendszerek és komponensek számára.

Általánosságban az allokációs folyamat a következő lépésekből áll:

- A rendszer tanulmányozása
- Azon területek megtalálása, ahol a terv és a hozzá tartozó RAMS karakterisztika információk elérhetők.
- Alkalmas súlyok hozzárendelése és
- Meghatározni a magasszintű követelményhez való hozzájárulását

[1]Reliability, Availability, Maintainability and Safety

A safety integrity level (SIL) egy diszkrét érték ami meghatározza a használandó módszereket, technikákat a véletlenszerű és szisztematikus hibák elkerülése érdekében. A SIL-ek koncepciója már több szabvány rendszerben ki lett fejlesztve. Ezek között legismertebb szabványok az IEC 61508, DEF-STAN-0056, EN 50126, EN 50128, EN 50129 és még sok más.

A SIL-nek két fő aspektusa van:

1. Egy cél hibaráta, amit a rendszernek nem szabad meghaladni, hogy tudja kezelni a véletlen hibákat

2. Módszerek és technikák halmaza, amit a szisztematikus hibákat kezeli

Itt fontos megjegyezni, hogy szoftverben csak és kizárólag szisztematikus hibákat vesznek figyelembe és nincs megadva cél hibaráta. Ez abból adódik, hogy a szoftverben nincs véletlenszerű hiba.

3.1.1. Különböző SIL-ek

A 3.1 táblázat példát ad a SIL-ek és a tűrhető hibaráta kapcsolatára, ahogy három szabvány, az IEC 61508, az EN 50129 és a DEF-STAN-0056 definiálja.

A tűrhető hibaráta (THR) egy eszköz veszélyes hibáinak maximális rátája, amit a szabvány definiál bizonyos safety integrity szinthez. Látni kell azt, hogy bár az IEC és EN szabványoknál azonosak a THR értékek, a DEF-STAN-0056-ban eltér. Ezért a szabványok közti átjárás nem mindig triviális. Attól még, hogy a THR értékek hasonlóak az IEC és EN szabványok között, az rendszer szintű hibaelkerülő módszerek különböznek, ezért ezek a SIL-ek sem ugyan azok.

SIL	IEC 61508/EN 50129	DEF-STAN-0056
1	$10^{-6}/h \leq \text{THR} < 10^{-5}/h$	Frequent $\approx 10^{-2}/h$
2	$10^{-7}/h \leq \text{THR} < 10^{-6}/h$	Probable $\approx 10^{-4}/h$
3	$10^{-8}/h \leq \text{THR} < 10^{-7}/h$	Occasional $\approx 10^{-6}/h$
4	$10^{-9}/h \leq \text{THR} < 10^{-8}/h$	Remote $\approx 10^{-8}/h$

3.1. táblázat. SIL értékek több szabvány és THR szerint

3.2. Allokációs módszerek

MIL-HDBK-388B[14] nyújt négy módszert az allokációhoz, melyek lentebb láthatók:

- Egyenlő elosztás módszer[2]
- ARINC[3] elosztás módszer
- „Feasibility of objective" módszer és
- AGREE[4] módszer

[2]Equal allocation technique
[3]Aeronautical Radio, Inc
[4]Advisory Group on Reliability of Electronic Equipment

Az egyenlő elosztás módszer és elosztási metodika, amely egyenlő részekre osztja fel a megbízhatósági követelményt a rendszer alrendszerei között. Ezt általában akkor használják, amikor nem áll rendelkezésre információ az alrendszerekhez. Az ARINIC módszer akkor alkalmazható, amikor csak az alrendszer meghibásodási ráta áll rendelkezésre. Az allokáció súlyozva van az alrendszer hozzájárulásával a rendszer hibára nézve. A harmadik módszer az alrendszer tervező megfelelő tapasztalata és tudása alapján jön létre. A módszer figyelembe veszi a rendszer komplexitását, környezetét és működési tartományát úgyan úgy, mint a hibarátát. Az AGREE technika az alrendszer összetettsége és az alrendszer hibájának a rendszerhibához való közreműködése alapján allokál (MIL-HDBK-388B, 1998).

3.2.1. Safety integrity szintek kombinációja

Ebben a részben a különböző szabványok SIL szintjeinek kombinációját mutatom be.

3.2.1.1. DEF-STAN-0056

A szabvány a következő szabályokat definiálja a 7.4.4. rész 5.8. táblázatában:

- Két SIL3 eszköz párhuzamos kombinációjaként létrejövő rendszer SIL4-es besorolású lesz.
- Két SIL2 eszköz párhuzamos kombinációjaként létrejövő rendszer SIL3-es besorolású lesz.
- Két SIL1 eszköz párhuzamos kombinációjaként létrejövő rendszer SIL2-es besorolású lesz.
- Két eszköz párhuzamos kombinációjaként - ahol az eszközök rendre SIL X és SIL Y besorolásúak - létrejövő rendszer SIL értéke SIL max(x,y).

Az olvasót a szabvány figyelmezteti, hogy ne keverje össze ezeket a szabályokat az EN 20129[2] által definiált safety integrity szintekkel.

Továbbá jelen esetben a "párhuzamos kombináció" azt jelenti, hogy a két eszköz vagy funkció úgy van társítva, hogy a veszélyes hiba kiváltásához mind a két eszköz hibája szükséges.

3.2.1.2. IEC 61508

A szabvány nem rendelkezik előre definiált szabályokkal, mint a fenti esetben, de ad némi lehetőséget magasabb integritási szint elérésére kombinációk által. Az általános szabály a következő (lásd IEC 61508-2, 7.4.4.2.4. rész):

Selecting the channel with the highest safety integrity level that has been achieved for the safety funciton under consideration and the adding N safety integrity levels to determing the maximum safety integrity level for the overall combination of the subsystem.

Itt N a párhuzamos kombinációban résztvevő elemek hardverhiba tűrése, azaz hány veszélyes hibát tud a rendszer tolerálni. Továbbá a rendszerek/elemek között is létezik megkülönböztetés, A és B típus.

Egy elem A típusúnak mondható, ha a biztonsági funkció eléréséhez a következők teljesülnek:

1. A komponens alkotórészeinek összes hibamódja jól körülhatárolt.
2. Hiba esetén a komponens viselkedése teljes mértékben meghatározható.
3. Létezik elegendő megbízható meghibásodási adat, ami bizonyítja az állított hibarátát.

Minden más elem/rendszer a B kategóriába kerül.

A követelményeknek való megfelelésből is látszik, hogy a szabvány nem ad egyszerű szabályokat a integritási szintek elosztásáról. Nem csak a rendszerek elrendezése és ez által a hardveres hibatűrése határozza meg a SIL-t, hanem még a rendszer biztonsági hiba hányada (Safe Failure Fraction [SSF]) is. Az SSF meghatározásának módját a szabvány C függelékében definiálja.

3.2.1.3. SIRF 400

A Sicherheitsrichtlinie Farhrzeug (SIRF) a németországi rendelet a vasúti járművek biztonságára. Németországban könnyű hivatkozni erre a dokumentumra, de az ország határain kívül nem biztosított az autómatikus megfelelése.

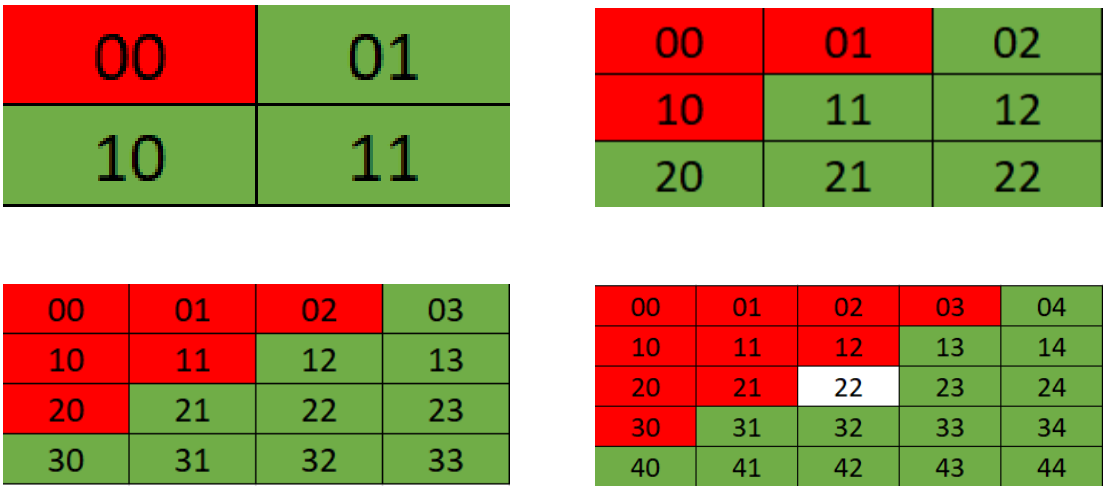
A dokumentum SIL allokáció problémájára a következő elveket adja.

Két alrandszer soros összeköttetése (például: hibafában VAGY kapuval összekötve) esetén, a legkisebb SIL érték határozza meg az összekapcsolt rendszer integritási szintjét.

A párhuzamos kombinációkhoz a következő szabályok adottak:

1. Egy SIL > 0 rendszer nem állítható össze SIL 0 elemekből.
2. Egy integritási szint elengedhető maximum egy szinttel egy ÉS kapu alatt.
3. Kizárás a 2. pont alól: Egy ág teljesen átveszi a biztonsági funkciót.
4. Kizárás a 2. pont alól: Common cause failure analízis kivitelezésre került.
5. A 4. pont esetében egy megfelelő szisztematikus módszert (FMEA, HAZOP, etc.) a hibafa legalsóbb szintjéig kell alkalmazni, hogy bebizonyosodjon a CCF kizárásának lehetősége.

Az 3.1. ábrán látható a SIRF által megengedett kombinációk. Az ábrákon zöld szín jelzi a megengedett, prios szín a tiltott kombinációkat és a fehér jelöli azokat, amikhez további elemzést kell végrehajtani, ami megmutatja az alegységek függetlenségét.



3.1. ábra. Megengedett kombinációk az integritás szinteknek megfelelően, sorrendben SIL1, SIL2, SIL3, SIL4 *Forrás*: SIRF 400

3.3. Top-down módszerek

3.3.1. Funkcionális analízis

A funkcionális analízis (FA) egy alapvető módszer a rendszer kritikus funkciói megértéséhez és tervezéséhez. Az FA elvégzése nélkülözhetetlen a RAMS menedzsmentben és a rendszertervezésben. A vizsgálat célja, hogy információt adjon arról, ami befolyásolja a rendszer funkcióit és alapot nyújtson a RAMS menedzsmenthez.

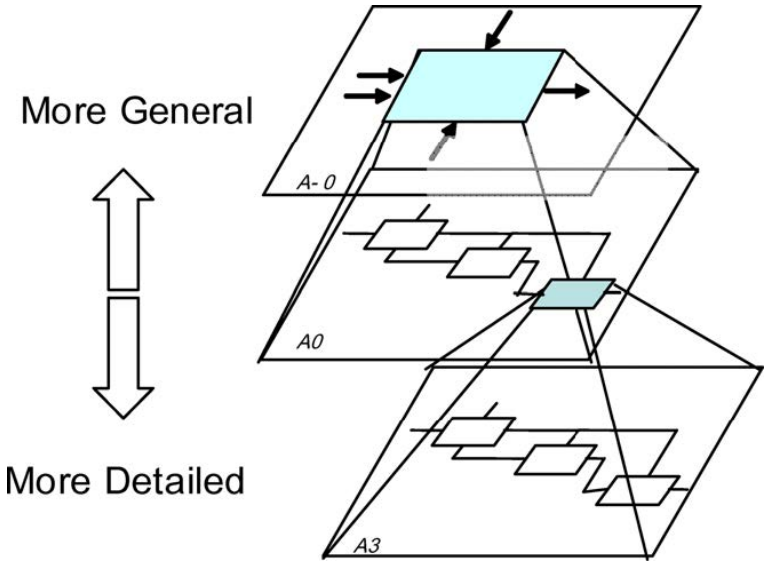
Az FA még a specifikáció, modellezés, szimuláció, validáció és verifikáció lépéseinél is alkalmazható. Ezért a funkcionális analízis gyakran fontos módszerként alkalmazzák a rendszer funkcionális struktúrájának meghatározására. A funkcionális analízist általában az alábbi két megközelítésben alkalmazzák:

- Struktúrált Analízis és Design módszer (SADT[5])
- Funkcionális Analízis Rendszer módszer (FAST[6])

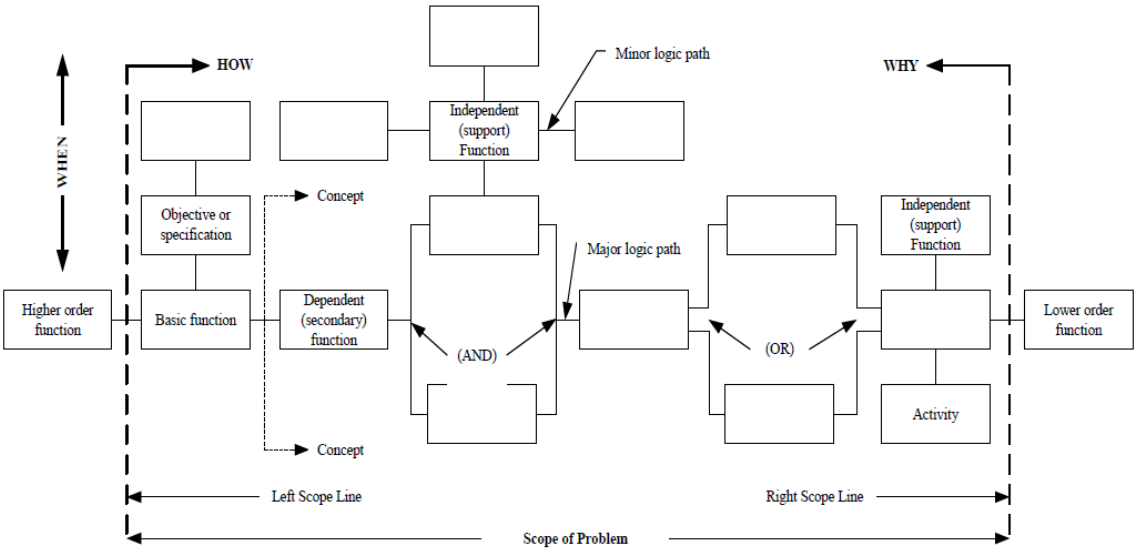
SADT-ot több iparágban is alkalmazzák. Ez egy diagramszerű koncepció, mely segítségével megérthető és leírhatók a rendszer funkcionális viselkedési és interfészei. A módszer számos elemet szolgáltat az aktivitások és adatfolyamok reprezentálására és nyilakat ezek kapcsolataihoz, ahhogy az alábbi 3.2 ábrán látható, ami egy példa az SADT-ra.

A FAST Charles Bytheway fejlesztette ki 1964-ben. Ezt a módszert is sok iparág használja. A FAST-ot azokban a szituációkban lehetséges felhasználni, ahol a funkciókat logikai sorozatban lehet ábrázoloni, ezáltal priorizálni őket és megvizsgálni a függőségeit. Ez a módszer nem alkalmas funkcionális problémák megoldására, inkább feltárni a rendszer alapvető funkcionális karakterisztikáit. Az 3.3 ábra egy példa a FAST modellre Kaufmann (1982) által.

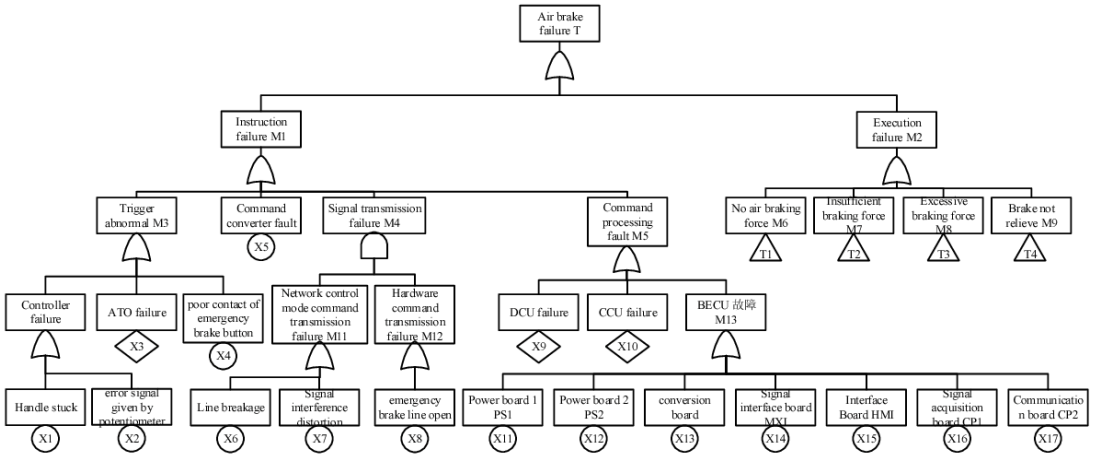
[5]Structured Analysis and Design Technique
[6]Functional Analysis System Technique



3.2. ábra. SADT modell (Forrás: Roh, 2007[20])



3.3. ábra. FAST modell (Forrás: Kaufmann, 1982, [12])



3.4. ábra. Egy hibafa példa pneumatikus fékrendszer meghibásodásához (Forrás: Long, 2017 [13])

3.3.2. Hibafa analízis

A Hibafa analízis (FTA[7]) egy szisztematikus, deduktív és logaikai módszer a rendszerhiba (Top event) okainak feltárására, modellezésére, vizsgálatára. Az FTA-t lehet az egyek legmegbízhatóbb eszköznek tekinteni a hiba eset logaikai kiértékelésében biztonsági és megbízhatósági szempontból. [11]

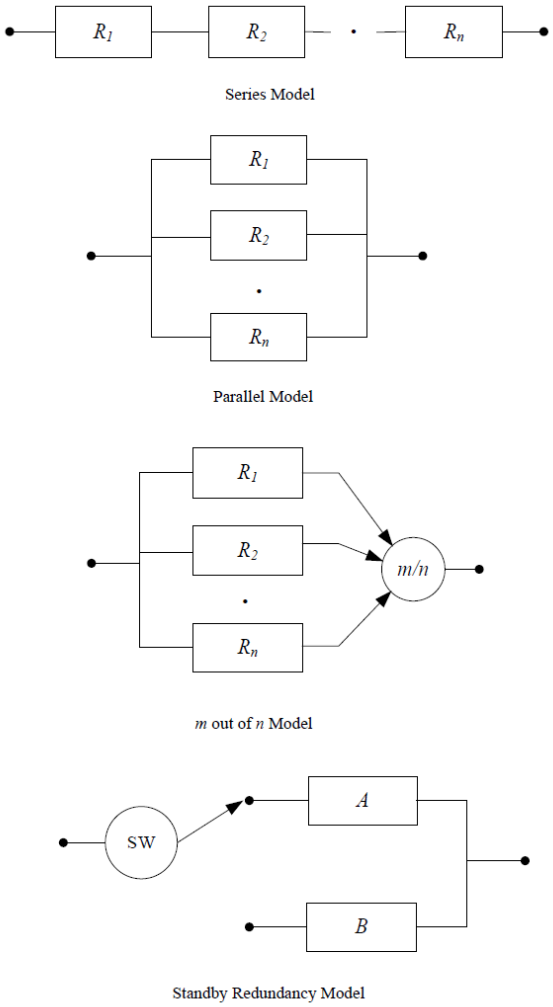
A hibafát H. Watson és Allison B. Mearns fejlesztette ki 1962-ben, akik együtt dolgoztak a US Bell Company laboratóriumában. Később a Boeing Company is elkezdte használni a módszert, hogy meghatározza a biztonsági faktorokat, melyek fegyverrendszerekre lehetnek hatással. Az 1960-as években a kereskedelmi repülés, '70-es években a nukleáris energiaipar, '80-as években a vegyipar, '90-es években közlekedési ipar is elkezdte használni a módszert biztonságosság és megbízhatóság felmérésére (Ericson, 1999).

Az analízis az előfordulható hibamódok egy részhalmazára fokuszál, különös tekintettel azokra, amik katasztrofális hibát okozhatnak. A kapuk (gate), események (event) és vágások (cut set) jelentik a legfőbb elemzési pontjait. A logikai diagramm - 'ÉS' és 'VAGY' kapuk - adja meg a FTA eredményét. A hibaesetek adják meg a kapuk bemeneteit és a vágások adják meg azoknak a hibaeseteknek halmazát, ami rendszerhibát okozhat. Az FTA-t szokás az FMECA[8]-val, Markov analízissel és ETA[9]-val együttesen használni, hogy elfedjék az FTA limitációit [9].

3.3.3. Megbízhatósági blokkdiagram analízis

A Megbízhatósági blokkdiagram (RBD[10]) egy vizuális elemzési módszer aminek segítségével könnyen reprezentálható a rendszer logikailag összekötött struktúrája. Az RBD blokkjai ábrázolják a rendszer eredményes működését. Az elemzés különböző szinten jelentkezhet, mind kvalitatív, mind kvantitatív formában. [19, 4]

[7]Fault Tree Analysis
[8]Failure Mode Effect and Criticallity Analysis
[9]Event Tree analysis
[10]Reliability Block Diagram



3.5. ábra. Különböző RDB modellek (Forrás: BS EN 61078, 2006)

A diagramm felépíthető egyenesen a rendszer funkcionális modelljéből, ami szisztematikusan megjeleníti a funkcionális utakat. Sok különböző rendszerkonfigurációt képes kifejezni, például, soros, párhuzamos, rendundáns, „standby" stb., ahogy az az 3.5 ábrán is látszik. Az RBD-t általában abban az esetben használják, amikor különböző változatait és komprumisszumait kell értékelni megbízhatósági és elérhetőségi szempontból.

3.3.4. Közös hibaforrás azonosítás

A rendszer biztonság fogalmának megalakulása óta nagy figyelem övezte a közös hibaforrásokat és azok azanosítását. Az első formalizált módszer 1998-ra tehető, amely amerikai Nukleáris Szabályzó Bizottság[11] számára készített tanulmányban szerepel. A közös hibaforrás azonosítására legelterjedtebb módszer a common cause failure analysis (CCFA). Ez az analízis szinte az összes a dolgozatban bemutatott vizsgálati módszernél elengedhetetlen, hiszen egy közös hibaforrás (CCF[12]) kihagyása a

[11]U.S. Nuclear Regulatory Commission
[12]Common Cause Failure

biztonsági analízis során A CCF egy egyfokú hiba, amely képes elrontani független redundás architektúrákat. [11]

Az analízishez elengedhetetlen a rendszert bármilyen logikai formában ábrázolni képes modell, mint például az FTA vagy az RBD.

3.3.4.1. Módszertan

A folyamat 8 lépésből áll.

1. Rendszer megállapítás
2. A rendszer kezdeti logikai modellezése
3. Átvilágító analízis
4. Részletes CCF analízis
5. Kimeneti kockázat értékelése
6. Korrekciós javaslatok
7. Veszélyek követése
8. A vizsgálat dokumentálása

3.4. Bottom-up módszerek

3.4.1. FMEA analízis

Az Hibamód és hatás analízis (FMEA[13]) egy biztonságossági és megbízhatőségi kiértékelő módszer, ami képes felmérni a rendszer összem komponensének összes potenciális hibamódját, ami kihathat az egész rendszer teljesítményére. A módszer továbbá azonosítja azokat a módszereket is, amikkel elkerülhetők a hibamódok és hogyan lehetséges csökkenteni azok hatását.

A módszert eredetileg FMECA[14] néven említették, amiben a ‚C' betű a hibamód kritikusságát jellemezte. Bár a két módszert gyakran szinonímaként használják, teljesen más a megközelítésük. Általában az FMEA-t a hibamód hatásának súlyosságát minősíti, míg az FMECA a hibamód frekvenciáját is megvizsgálja a súlyosság mellett. A súlyosság és a frekvencia kombinációját a rendszer kritikusságnak vagy kockázatának nevezik [15].

A módszer során minimum a következő nyolc információt kell megállapítani:

1. Hibamódok (Failure mode)
2. A hibamód hatása a rendszerre
3. A hibamód miatt bekövetkezett rendszerszintű hiba
4. A veszélyek baleseti hatása

[13]Failure Mode and Effect Analysis
[14]Failure Mode Effect and Criticality Analysis

5. A hibamód és/vagy veszély okozati tényezőit
6. Hogyan lehet a hibamódot detektálni
7. Javaslatok
8. A felderített veszély kockázatát

A módszert több szempontból is el lehet végezni. Ez lehetnek Funkcionális megközelítés, Struktúrális megközelítés és a „hibrid" megoldás. Az első megközelítésben a funkciók céljának lehetséges hibás működését veszi figyelembe. Ez a módszer alkalmazható szoftverek esetében is.

A második megközelítés leginkább hardver elemeken végzett lehetséges hibamódokra öszpontosít. A „hibrid" megközelítés először a funkcionális analízissel kezdődik, aminek fókusza átvált a hardverre [11].

Lehetséges példák a funkcionális hibamódokra:

- A funkció nem működik
- A funkció nem megfelelően működik
- A funkció idő előtt hajtódik végre
- A funkció hibás vagy félrevezető információt szolgáltat
- A funkció nem hibásodik meg biztonságosan

Lehetséges hardver hibamód kategóriák:

- Teljes meghibásodás
- Részleges meghibásodás (például: tolerancián kívül)
- Időszakos meghibásodás

Lehetséges hardver hibamódok:

- Szakadás
- Rövidzárlat
- Tolerancián kívül
- Szivárgás
- Meleg felület
- Elhajlás
- Túl/alulméretezett
- Megrepedt
- Rideg
- Elmozdult

- Korrodált
- stb.

Lehetséges hibamódok szoftvereknél:

- A szoftver funkció meghibásodik
- A funkció hibás eredményt szolgáltat
- A funkció idő előtt meghívódik
- Elküldetlen üzenetek
- Túl korán/későn küldött üzenet
- Hibás üzenet
- Megáll vagy összeomlik a szoftver
- Belső kapacitásoknál többet igényel a szoftver
- Szoftver „startup" hiba
- Lassú válaszidő

3.4.2. HAZOP analízis

A Hazard and operability study (HAZOP) analízis egy szisztematikus vizsgálat, ami feltárja és tanulmányozza egy rendszer potenciális veszélyeit és üzemeltetési problémáit. Rendezett, struktúrált és módszeres folyamatot követ[11].

A HAZOP-ot az angol Chemical Industry Insitute formalizálta a '70-es években. A módszer széleskörben elterjedt számos biztonságkritikus iparágban, mint a vegyipar.

A módszertan néhány útmutató szó segítségével próbálja rávezetni a vizsgálót a problémás részekre. Ilyen útmutató szavak lehetnek például: 'Nem', 'Több', 'Kevesebb', 'Fordítva' stb., mint az látható a 3.2. táblázatban. A HAZOP módszer leghatékonyabb a részletes terv kidolgozása után, mert ilyenkor már működtetési problémákat is feltár. A 3.2 táblázat egy vonat ajtó működési problémáit tárja fel egy peronnál HAZOP segítségével.

3.4.3. LOPA

Layer of Protection Analysis-t (LOPA) először az 1990-es évek végén kezdték el alkalmazni a vegyiparban. Ahogy a módszert egyre szélesebb körben alkalmazták, az AIChE Center of Chemical Process Safety (CCPS) elkezdett irányelveket kiadni hozzá. Később más szervezetek is elkeztek a LOPA-ra hivatkozni, mintpéldául az IEC[15] vagy az ISA[16] [26].

A layer of protection analysis megfeleltethető az Event Tree Analysis (ETA) egy megfelelő adaptációjának[17], lásd: 3.6. ábra.

[15]International Electrotechnical Commission
[16]International Society of Automation

Útmutató	Eltérés	Ok	Okozat
Nem	Az ajtó nem nyílik	Hibás mechanizmus	Nem tudnak leszállni az utasok
Több	Az ajtó túl korán nyílik	Kezelő hibázik	Lehetséges sérülés
Kesevebb	Csak egy ajtó nyílik ki	Hibás mechanizmus	Korlátozott leszállás, lehetséges sérülés
Ugyan úgy	A vonat mindkét oldalán nyílik az ajtó	Hiba a vezérlőben	Lehetséges sérülés, ha a rossz oldalon szállnak le
Más mint	Rossz oldalon nyílik az ajtó	Vezérlő hiba	Lehetséges sérülés, ha a rossz oldalon szállnak le

3.2. táblázat. Egy példa a HAZOP használatára

A LOPA analízist általában közvetlenül a HAZOP tanulmány után készítik el, de még a hibafa analízis előtt.

3.4.3.1. LOPA koncepciója

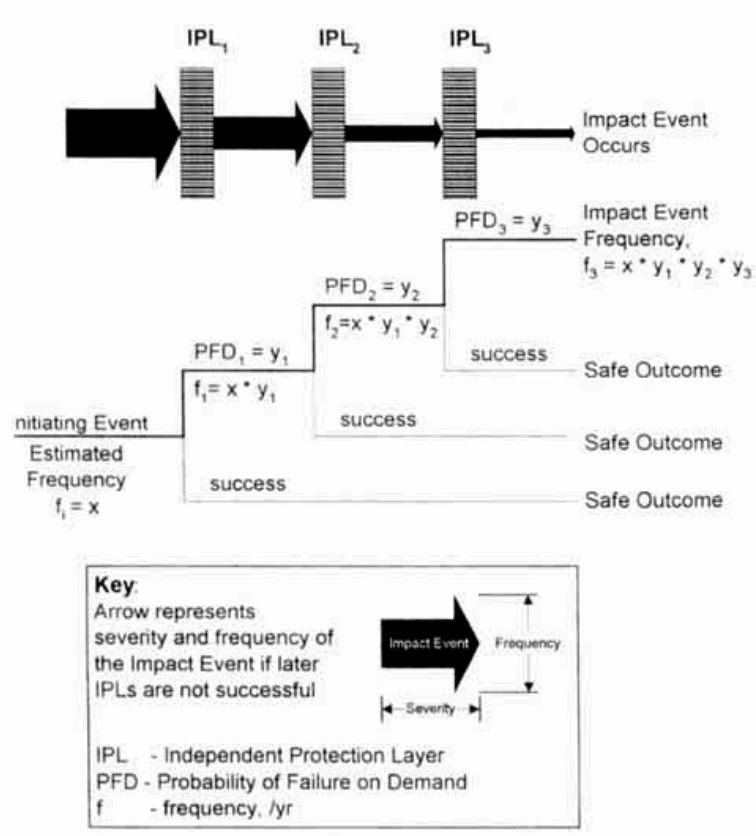
A LOPA koncepciója összefoglalva:

1. Megtalálni azokat az eseményeket, amelynek a külvilágra hatása van. Meghatározni ezek hatását(emberek, környezet, tulajdon)
2. Felsorolni a ezeknek az eseményeknek a kezdeti okát.
3. Megbecsülni a kezdeti okok frekvenciáját.
4. Minden ok-okozati párra felsorolni a független védelmi rétegjét (IPL[17]).
5. Meghatározni a hiba valószínűségét minden IPL-nek.
6. Kiszámolni a mérsékelt előfordulási frekvenciát az összes ok-okozati párra.
7. Összevetni a kapott frekvenciát az előre definiált tűrhető veszéllyel.

Ha mindezek után a kapott érték nem teljesíti a kritériumot az alábbi opciókat lehet végrehajtani:

- További rétegeket adunk a rendszerhez.
- Növeljük valamelyik réteg SIL szintjét (azaz csökkentjük annak frekvenciáját)
- Újratervezzük a folyamatot vagy
- még részletesebb vizsgálatot folyatatunk, pédául: Hibafa Analízissel.

[17]Independent Protection Layer



3.6. ábra. LOPA analízis esemény fával ábrázolva (Forrás: [6])

4. fejezet

Esettanulmány

4.1. A tanulmány háttere

Az esettanulmány során egy kitalált, de mégis valósághű vasúti fékrendszert tervezek és elemzem biztonsági szempontból.

A vasútipart és ezzel együtt a vasútifék-technológiát az utóbbi időben rohamos fejlődés határozta meg. Számos működési elv elérhető az iparágban (pneumatikus, hidraulikus, elektro-pneumatikus, elektro-hidraulikus, elektromágneses), amelyeknek mind meg van a maga előnye és hátránya.

Ebben a dolgozatban egy összetett integrált fékrendszer megoldást szeretnék modellezni, mely rendelkezik egy fékvezérlő berendezéssel. Ezért az elavultnak számító és mára leginkább csak a vasúti teherszállításban - az egyszerűsége és költséghatékonysága miatt - használt pneumatikus és a szintén tisztán fizikai elven működő hidraulikus rendszereket nem találtam alkalmasnak a dolgozat témájához.

Napjainkban fontos téma, többek között a globális felmelegedés és a CO_2 kibocsátás visszaszorítása - melyek részletei és elemzése nem képezik ennek a dolgozatnak részét - miatt, a tömegközlekedés. A vasútipar emberek szállítmányozására alkalmas része is több alrészre bontható, nagysebességű(>300 km/h)/intercity vonatok, regionális/ingázó vonatok (pl: Budapesti HÉV), metró, könnyű vasúti vonatok/villamosok.

A dolgozat során egy modern alacsonypadlós városi tömegközlekedésre alkalmas villamos rendszerén keresztül szeretném bemutatni a modell alapú rendszertervezés (Model-based Systems Design, MBSD) módszertanait és az elkészült rendszer biztonsági és megbízhatósági analízisét. Mivel az alacsonypadlós villamosokon véges hely áll rendelkezésre, ezért egy kompakt megoldásra van szükség. Továbbá, biztosítani kell bármely közlekedési helyzetben a szerelvény biztonságos és optimális lassulását, megállását.

4.2. Vasúti jármű fékrendszer

A vasúti járművek fékei rendkívül összetett folyamatot alkotnak és specifikusak a vasúti járművekre. A fékrendszer egy fontos biztonsági funkció, mely szabályozza a jármű sebességét és megállítja egy fix helyen, mint például egy állomásnál [18].

Egy vasúti fékrendszernek a következő célokat kell teljesíteni:

- Lassítani vagy megállítani a mozgó vonatot

- Biztosítani az álló járművet
- Kontrollálni a jármű sebességét lejtőn

Ezekhez számos funkciót kell teljesítsen a rendszer, melyek a kövezkezők:

- üzemi fék
- vészfék
- biztonsági fék
- biztosító fék
- parkoló fék
- opcionálisan kerékcsúszás prevenciós rendszer (WSP[1])

4.2.1. Üzemi fék

Az üzemi fék az elsődleges fékrendszer normál üzemi állapotban. Ezt a rendszert általában a jármű vezetője és/vagy a járművet vezető autómatika kezeli, hogy az általuk kívánt sebességre szabályozzák a vasúti szerelvényt.

4.2.2. Vészfék

Ezen funkció legfőbb célja az utasok, személyzet és a vasutat nem használók biztonságának maximalizálása. Továbbá ez a funkció képes a lehető leghamarabb nyugalmi állapotba hozni a szerelvényt.

4.2.3. Biztonsági fék

Európában és a világ számos pontján kötelező olyan berendezéssel ellátni az új járműveket, amely a szerelvény esetleges menetközben több részre szakadásakor a jármű összes részét biztonságosan megállásra kényszeríti. Ezt a funkciót nevezik biztonsági fékmechanizmusnak.

4.2.4. Biztosító fék

Ez a funkció felel a jármű egyhelyben tartásáért, amikor megáll a jármű egy állomáson.

4.2.5. Parkoló fék

A parkoló fék felel a jármű helyben tartásáért, miközben a jármű üzemen kívül van.

4.2.6. Kerékcsúszás prevenciós rendszer

A WPS[1] egy olyan rendszer, amely optimalizálja a fékteljesítményt és védelmet nyújt a kerék és a sín sérülése ellen gyenge súrlódási viszonyok között.

[1]Wheelslide Protection System

5. fejezet

Modellezés

5.1. Követelmény modellezés

A modellezendő rendszerhez alapvetően EN 13452[7] szabvány első részében található funkcionális követelményeket vettem figyelembe. Az 5.1 ábrán látható a követelmények modellje. Ezen megjelenik a öt fő funkció, amit a rendszernek teljesítenie kell.

5.2. Funkcionális dekompozíció

A 5.2. ábrán látható a funkcionális dekompozíciójának block definition diagramja. Ezen látható, hogy a fékrendszer több elemet is támogat a 4.2. részben taglalt funkciók közül. A rendszer a következő öt funkciókkal rendelkezik, ahogy az a 5.2. ábrán is látható: (1) üzemi fék (service brake), (2) vészfék (emergency brake), (3) biztonsági fék (security brake), (4) parkoló fék (parking brake) és (5) kerékcsúszás gátlás (wheelslide protection). Továbbá az ábrán az is látható, hogy a fékrendszer képes forgóvázra nehezedő súly által szabályozni a fékezési erőt.

A 5.3. ábrán látható a rendszer belső felépítése (IBD[1]). Az ábra tartalmazza és definiálja az alrendszerek kapcsolatát, továbbá leírja a rendszer külső csatlakozási pontjait portok által.

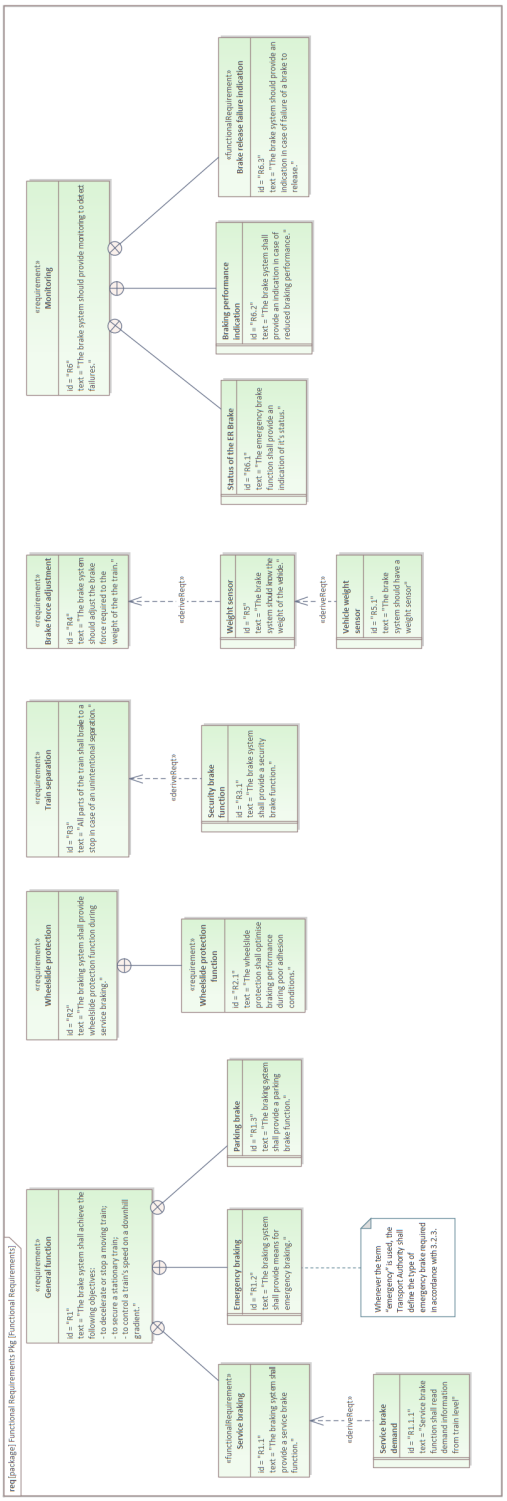
5.2.1. Üzemi fék

Az dekompozíciós folyamatot az üzemi fék alrendszeren folytatva a 5.4. ábra mutatja az üzemi fék funkcionális felbontását/BDD[2]-jét. Az ábrán látható, hogy ez egy vezérlő funkció ezért megjelenik a vezérlő-rendszer-visszacsatoló hármas a modellben. Továbbá az is látszik, hogy a vezérlő funkció egy összetett eleme az alegységnek.

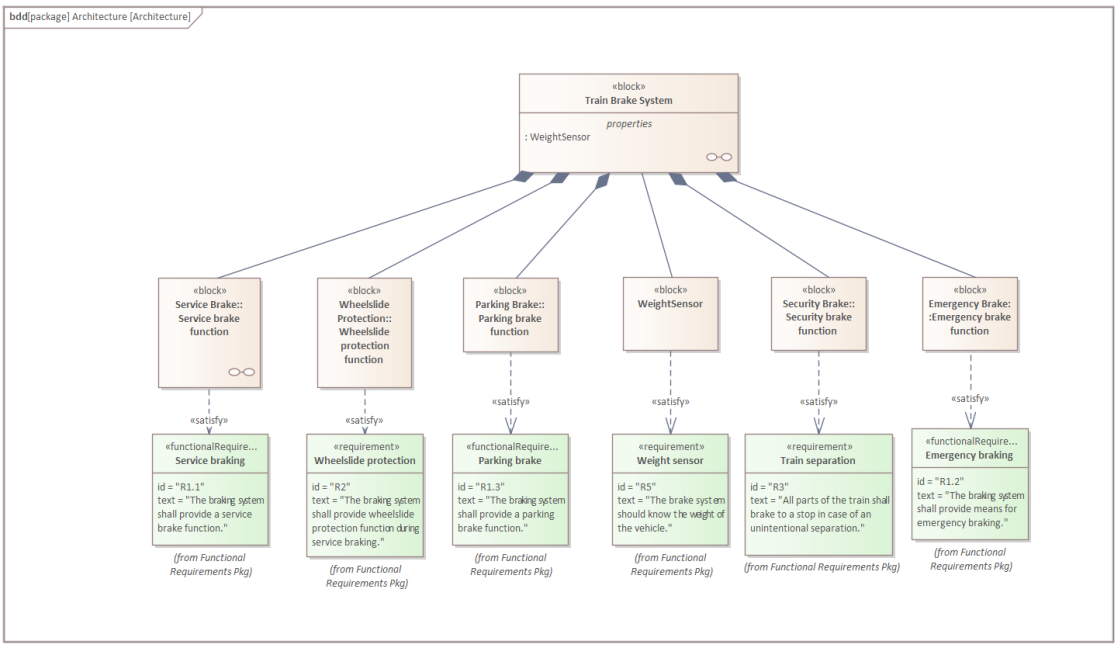
5.3. Platform modellezés

Ebben a részben a fentebb elkészített funkciónális modellhez tartozó platform modellt fogom bemutatni. SysML-ben platform modelleket használunk arra a célra,

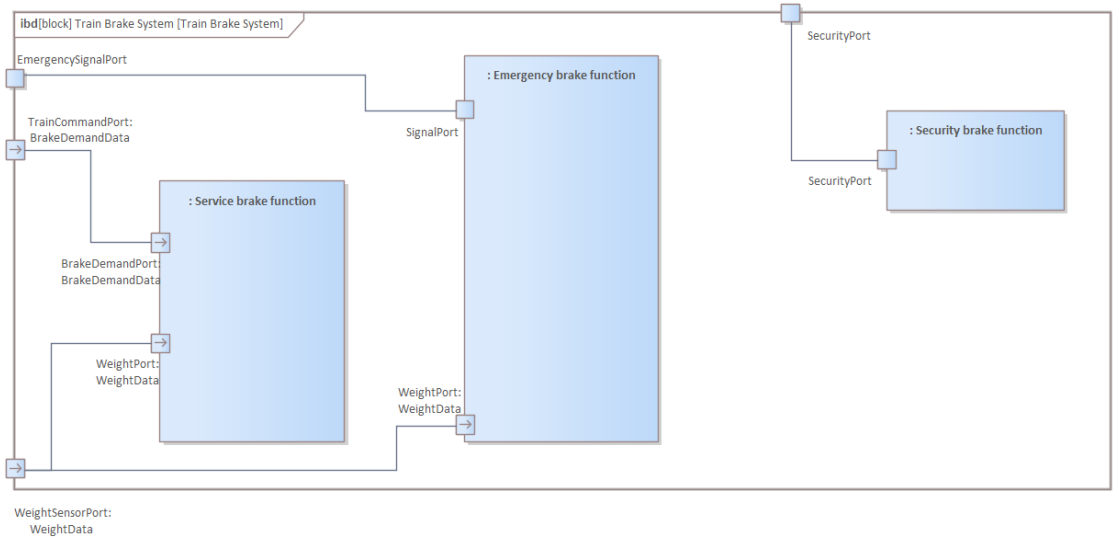
[1] internal block diagram
[2] Block Definition Diagram



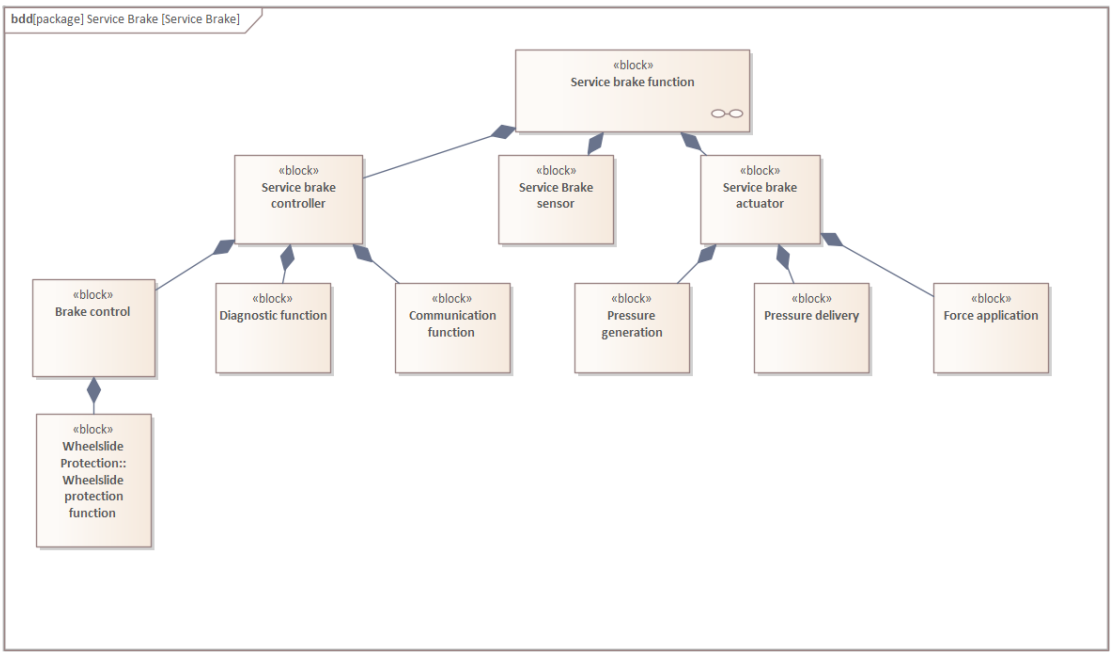
5.1. ábra. A rendszer funkcionális követelményinek modellje SysML-ben.



5.2. ábra. A tervezett fékrendszer funkcionális dekompozíciója



5.3. ábra. A fékrendszer belső felépítése



5.4. ábra. Üzemi fék blokk definition diagramm-ja.

hogy a megtervezett funkciókat ténylegesen hardver/softver elemekhez allokáljuk. Ezek a modellek már a valódi fizikai alkatrészeket, illetve ezek kapcsolátát reprezentálják. Ebben a fázisban általában Bottom-up tervezési elvet használnak, hiszen ez a folyamat nagyon hasonlít arra, amikor egy nyomtatott áramkört tervezünk és inkább alkatrészkönyvtárakból válogatnak a mérnökök.

5.3.1. Aktuátorok

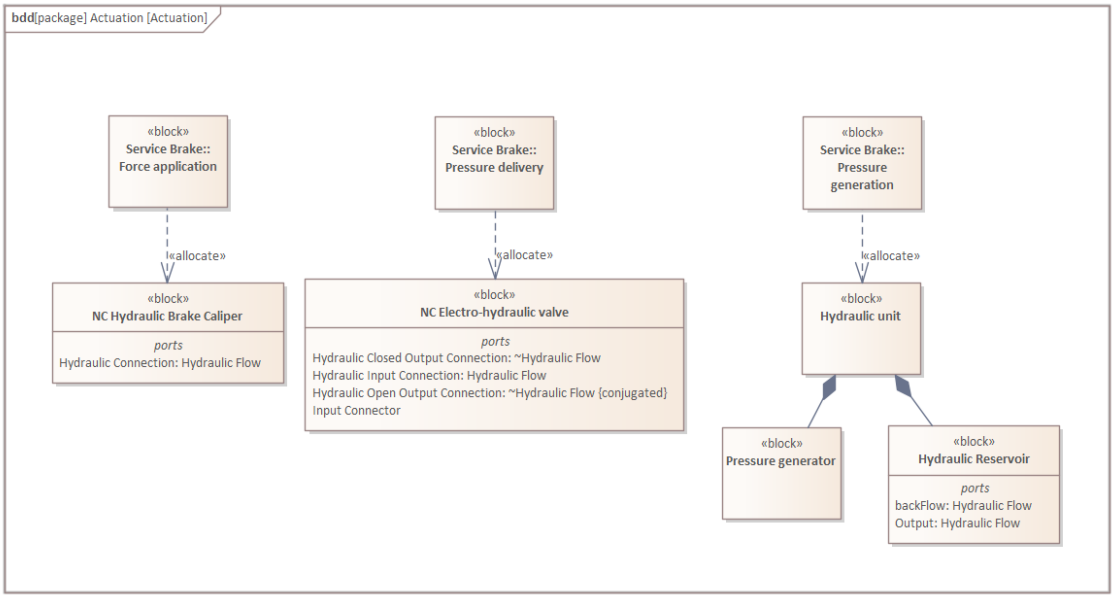
A 5.5. ábrán láthatók a fékrendszer azon aktuátorai, melyek részt vesznek a fékezés folyamatában. Az ábrán látható NC[3] jelölés megjelenik mind a vezérlő szelepnél (valve), mind a fékollónál (brake caliper). Az előbbi esetében ez azt jelenti, hogy ameddig nem kap megfelelő feszültséget a bemeneti csatlakozóján addig nyitva tartja a hidraulikus folyadék útját a gyűjtőtartály felé, ezzel csökkentve/elengedve a hidraulikus rendszerben lévő nyomást. A fékolló esetében pedig azt jelenti, hogy egy olyan mechanikai megoldást alkalmaz, amely rugós előfeszítéssel fékezi a hozzá tartozó féktárcsát. Az eszközt hidraulikus nyomás segítségével lehet leoldani/lazítani a féktárcsáról, ezáltal a rendszer örökölten képes támogatni a parkoló fék funkciót.

Ezen alkatrészek segítségével már az összes olyan funkciót meg lehet valósítani, ami a kívánt fékezési erőt képes átadni az adott tengelyre.

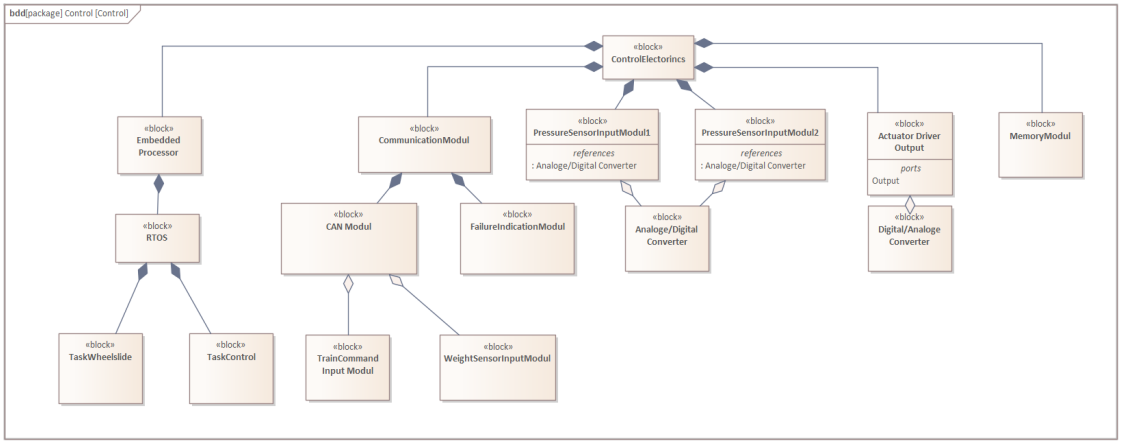
5.3.2. Elektronikai vezérlő

Az elektro-hidraulikus fékrendszer elengedhetetlen rész a vezérlő elektronika. Ez a részegység felelős a hidraulikus rendszer irányításáért, ellenőrzéséért és a hibajelzésért.

[3]Normally Closed



5.5. ábra. A fékrendszer aktuátorainak platform modellje.



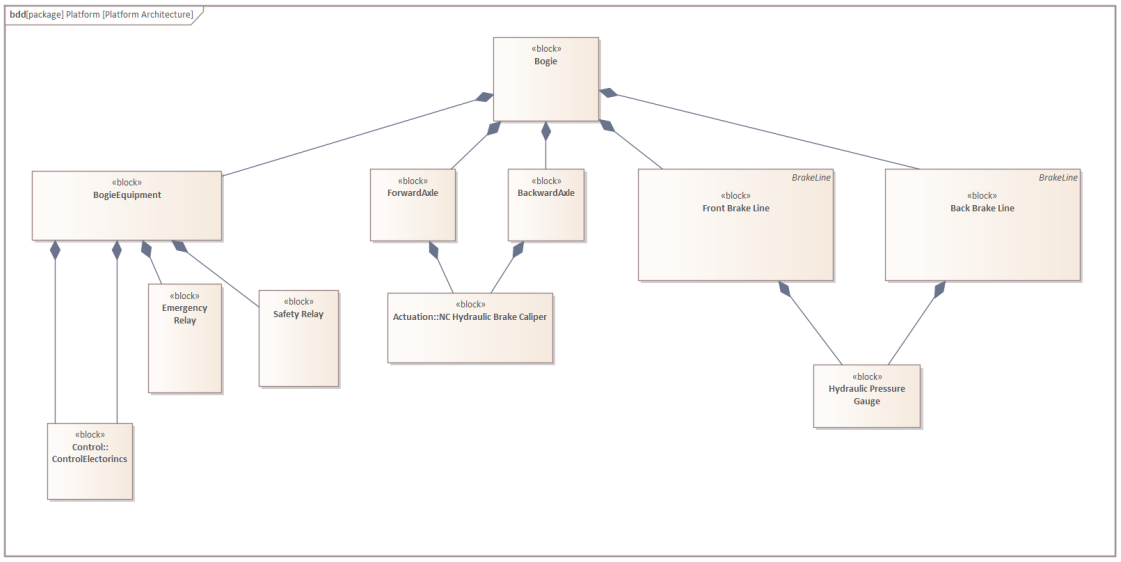
5.6. ábra. A vezérlő elektronika platform modellje bdd-n bemutatva.

Általában ez az egység képezi a forgóvázon elhelyezett fékrendszer legösszetettebb részét. Továbbá itt található meg a legtöbb biztonság-kritikus funkció is. A 5.6. ábrán látható a vezérlőelektronika blokkdefiníciós diagrammja.

Az ábrán látható, hogy a rendszer nem annyira összetett, mint a valóságban, de szerepelnek rajta olyan elemek, melyek megjelennek egy tényleges projektben. Ezek például az analóg-digitális és digitális-analóg átalakítók, beágyazott vezérlő processzot valósidejű operációs rendszert futtatva, illetve a hozzá tartozó memória illetve kommunikációs modulok.

5.3.3. Platform architektúra modell

Végezetül elkészítettem a fentebb említett kisebb egységek összekapcsolásával/kombinálásával az egy forgóvázon (bogie-n) elhelyezhető, kompakt fékrendszert. Mint az



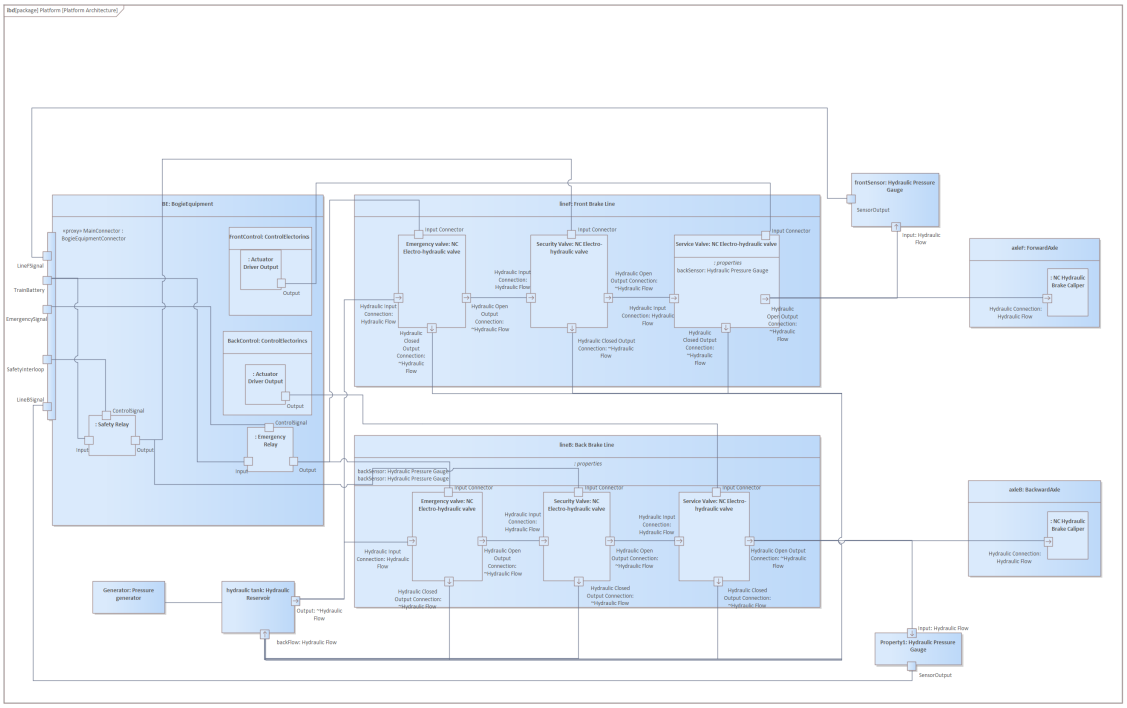
5.7. ábra. A fékrendszer platform modelljének architektúrája bdd-n ábrázolva.

a 5.7. ábrán látható, a fékrendszer két független fékkörrel rendelkezik, amely képes a forgóvázon lévő mind a két tengelyt fékezni.

Ezen redundancia alkalmazásával a rendszer képes elegendő fékerőt generálni, még ha esetlegesen az egyik fékkör meghibásodna.

A 5.8. ábra szemlélteti a rendszer összeköttetéseit, az alkatrészek kapcsolatát. Ezen már megjelenik a teljes mértékben összekapcsolt hidraulikus rendszer a két függetlenül vezérelt hidraulikus körrel, illetve az úgynevezett BogieEquipment (BE), ami az iparágban a forgóvázra felszerelhető egységet jelenti.

A BE tartalmazza általában a vezérlő elektronikát és a hozzá tartozó csatlakozási pontokat is. Ezt a fentebb említett ábra is remekül szemlélteti, hiszen ebben az egységben helyezkedik el mind a két vezérlő elem, illetve a biztonsági és vészfék irányíttó kapcsoló is.



5.8. ábra. A fékrendszer fizikai összeköttetései, alkatrészeinek kapcsolata ibd-n ábrázolva.

6. fejezet

Safety analízis

A dolgozat során elkészített rendszer terv csak akadémiai célokat szolgál, ezért nem követi teljes mértékben a valóságot. Teljes mértékben kielégítő biztonsági vizsgálatot ezért nem lehet végezni a rendszeren. A következő részekben inkább szeretném bemutatni egyes elemzési módszerek lényegét, alkalmazhatóságát mintsem egy valós projekt szerinti precíz megvalósítsát.

Mivel a biztonságosság kiemelten fontos témakör az iparágban, ezért az elemzésben a valósághoz hasonló értékek szerepelnek, de ezen értékek kitaláltak és reprezentatív jellegűek. Az analízis során feltárt kockázatok besorolását az EN 50126[8] első részében leírt kockázat mátrix kalibrációs táblázatai szerint határoztam meg.

A frekvenciák besorolásához a 6.1. táblázatot készítettem el. Ennek segítségével besorolhatók egyes kvantitatív értékek az elfogadási mátrixban.

Továbbá a 6.2 és a 6.3 segédtáblázatok alapján már meghatározható az a táblázat, amely a balesetek súlyossága és a hiba előfordulásának gyakorisága alapján meghatározza a kockázat elfogadásának lehetőséget. Ezt a táblázatot reprezentálja a 6.4 táblázat.

Az elemzések további szakaszaiban ezen táblázatok felhasználása szerint lesznek meghatározva az előforduló hibák. Továbbá feltételezhetjük, hogy a rendszer várható élettartama 30 év és átlagosan évente 5 000 órányi igénybevételnek lesz kitéve.

6.1. HAZOP analízis

A vizsgálatot HAZOP tanulmány készítésével kezdtem. Ez alkalmas a rendszer platform modellje alapján előre meghatározott módszertan szerint szisztematikusan eltárni az adott alrendszerek tervezettől való eltérő viselkedéseinek feltárására.

A vizsgálat segéd szavak segítségével vezeti rá az elemző (csapat) gondolkodását a lehetséges eltérésekre. A módszertan által nyújtott lehetséges szavak csak egy részét felhasználva, a következő iránymutató szavak lettek felhasználva a dolgozatban: (1) NEM (NO), (2) KEVESEBB (LESS), (3) TÖBB (MORE).

Ezután két alrendszert vizsgáltam a módszertan szerint, ezek pedig a hidraulikus fékolló (Hydraulic Caliper) és a vezérlő elektronika (Control Electronics).

A HAZOP tanulmány eredményessége nagyban függ az azt végrehajtó csapat kreativitásán, ezért nem feltételezhető az adott egység minden egyes hibaforrásának észlelése/feltárása.

Frekvencia szint	Leírás	Frekvencia példa egy 24 órában működő eszköznél	Frekvencia
Gyakori	Az esemény gyakran bekövetkezik	Több mint egyszer 6 hónapos időszak alatt	$f \leq 1 \times 10^{-3}$
Valószínű	Az esemény várhatóan többször bekövetkezik	Hozzávetőlegesen egyszer 6 hét és egy év között	$1{\times}10^{-3} < f \leq 1{\times}10^{-4}$
Alkalmi	Az esemény több alkalommal bekövetkezhet	Hozzávetőlegesen egyszer egy év és 10 év között	$1{\times}10^{-4} < f \leq 1{\times}10^{-5}$
Ritka	Valószínű, hogy bekövetkezik valamikor a rendszer élettartama során	Hozzávetőlegesen egyszer 10 év és 1 000 év között	$1{\times}10^{-5} < f \leq 1{\times}10^{-7}$
Valószínűtlen	Velószínűtlen a bekövetkezés, de megtörténhet	Hozzávetőlegesen egyszer 1 000 év és 100 000 év között	$1{\times}10^{-7} < f \leq 1{\times}10^{-9}$
Erősen valószínűtlen	Az esemény vélhetően egyszer sem fog bekövetkezni	Hozzávetőlegesen egyszer 100 000 éveben vagy kevesebbszer	$1 \times 10^{-9} < f$

6.1. táblázat. A veszély besorolási mátrix frekvencia tartomány kalibrációja. Saját adatok, a [8] alapján.

Súlyossági kategória	Következmények az emberekre / környezetre	Következmények a szolgáltatásokra
Katasztrofális	Emberek tömegét befolyásolja és többek halálához vezethez és/vagy súlyos környezeti károsodás	-
Kritikus	Emberek kis számát befolyásolja és legalább egy halálesetet okoz és/vagy nagy környezeti károsodás	Egy fontos rendszer elvesztése
Marginális	Nincs lehetőség halálesetre, cask súlyos vagy könnyű sérülések és/-vagy kis környezeti károsodás	Súlyos rendszer sérülés
Jelentéktelen	Lehetséges könnyű sérülés	Jelentéktelen rendszer sérülés

6.2. táblázat. Súlyossági kategóriák, az EN 50126-1 alapján.

Kockázat elfogadási kategória	Végrehajtandó intézkedések
Tolerálhatatlan	A kockázatot meg kell szüntetni
Nem kívánatos	A kockázatot csak abban az esetben lehet elfogadni, ha annak csökkentése nem lehetséges
Tolerálható	A kockázat tolerálható és elfogadható megfelelő ellenőrzéssel (például: karbantartási útmutatók vagy szabályok)
Elhanyagolható	A kockázat minden további nélkül elfogadható

6.3. táblázat. Kockázat elfogadási kategóriák, az EN 50126-1 alapján.

Előfordulási frekvencia	Kockázat elfogadási kategória			
Gyakori	Nem kívánatos	Tolerálhatatlan	Tolerálhatatlan	Tolerálhatatlan
Valószínű	Tolerálható	Nem kívánatos	Tolerálhatatlan	Tolerálhatatlan
Alkalmi	Tolerálható	Nem kívánatos	Nem kívánatos	Tolerálhatatlan
Ritka	Elhanyagolható	Tolerálható	Nem kívánatos	Nem kívánatos
Valószínűtlenű	Elhanyagolható	Elhanyagolható	Tolerálható	Nem kívánatos
Erősen valószínűtlen	Elhanyagolható	Elhanyagolható	Elhanyagolható	Tolerálható
	Jelentéktelen	Merginális	Kritikus	Katasztrofális
	A baleset súlyossága			

6.4. táblázat. Kockázat elfogadási mátrix.

Az általam elvégzett vizsgálat során a 6.5. táblázatban látható potenciális eltérésekre jutottam.

6.2. LOPA analízis

A LOPA vizsgálat során a következő forgatókönyvet fogom elemezni: A kerékcsúszás prevenciós modul túl sokáig (> 3 sec) tartja fékezetlen állapotban a rendszert miközben fékezési parancs van kiadva.

HAZOP tanulmány során derült fény erre a potenciális hibára. A tanulmány alapján kijelenthető, hogy a eset kiváltó hiba potenciálisan a kerékcsúszás prevenciós alrendszer beragadása egy olyan állapotba, ahol jelentősen csökkentett fékerő kerül kivezérlésre a végős beavatkozóhoz.

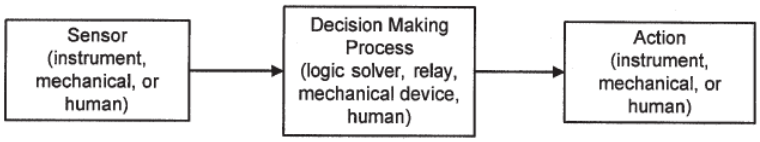
Ez különböző módokon lehetséges, amiknek további elemzése nem célja a vizsgálatnak, de lehet processzor, memória esetleg a vezérlést végrehajtó hardver hibája. Továbbá tudjuk, hogy ez a hiba $4 \times 10^{-4} 1/h$ frekvenciával fordul elő.

A lehetséges következmények között feltárva lett, olyan kimenetel is, hogy a hiba akár halálesethez is vezethet. Ezért a 6.2 táblázat alapján a hiba *Kritikus* besorolást kap. A megadott hibarátát figyelembe véve a 6.1 táblázat szerint az előfordulás besorolása *Alkalmi* kategóriájú.

A fentiek alapján a következő megállapítás fogalmazhatódhat meg az hibamód elfogadhatóságáról: A kapott besorolások alapján bármilyen enyhítő körülmény nélkül a kockázat elfogadási mátrix (lásd: 6.4. táblázat) alapján *Nem kívánatos* besorolást kap. Ez csak akkor elfogadható, ha azt lehetséges tovább csökkenteni.

Item	Guide word	Deviation	Cause	Consequence	Existing controls
Hydraulic Caliper	NO	No brake force	Caliper failure	Longer braking distance / possible crash with traffic	Recommended service interval / routine checks
	LESS	Reduced brake force	Worn out brakepads	Longer braking distance / possible crash with traffic	Recommended service interval / routine checks
	LESS	Reduced brake force	Control loop failure	Longer braking distance / possible injury to multiple people	-
	MORE	More brake force	Failure of pressure generation	Possibility of train stuck on track / minor injuries	-
Control Electronics	NO	No input voltage	Train battery line failure	Train stuck on track	-
	MORE	Higher input voltage than specified	Train battery line failure	Control electronics power supply failure	Over voltage protection
	MORE	Higher brake demand than requested	Control output stuck at low	Possibility of train stuck on track / minor injuries	Under voltage protection
	LESS	Lower input voltage than specified	Train battery line failure	Possibility of train stuck on track / minor injuries	-
	LESS	Lower brake demand than requested	Control output stuck at high	Longer braking distance / possible injury to multiple people	Error signaling
	LESS	Lower brake demand than requested	Wheelslide protection lowers the brake demand for a long time	Longer braking distance / possible injury to multiple people	WSP watchdog

6.5. táblázat. HAZOP vizsgálat a hidraulikus fékolló és vezérlő elektronika komponensekre.



6.1. ábra. Egy aktív IPL felépítése. Forrás: [5]

6.2.1. Független Védelmi Rétegek vizsgálata

Ahhoz, hogy eszközt, rendszert vagy funkciót független védelmi rétegnek (továbbiakban IPL[1]) lehessen tekinteni a következőnek kell teljesülni[5]:

- *hatékonyan* megakadályozza következményt ha úgy működik, ahogy tervezték
- *független* a kezdő/kiváltó eseménytől és a többi IPL összes komponensétől, ami szerepel a forgatókönyvben
- *auditálható*, az elvárt viselkedés valamilyen módon validálható/bizonyítható

Az IPL-eknek két altípusát különböztetjük meg: (1) Passzív IPL, (2) Aktív IPL.

A passzív IPL-eknek nem szükséges, hogy beavatkozzanak a folyamatba ők eredendően csökkentik a kockázatot. Az irodalomban számtalan példa található a kémiai iparágban használható passzív védelmi mechanizmusokról, de a jelen problémához nem alkalmazható ilyen elven működő eszköz.

Az aktív IPL-ek valamilyen érzékelő segítségével képes egyik állapotból a másikba kerülni ezáltal megváltoztatva a folyamatot. Ezek egy lehetséges felépítését a 6.1. ábra szemlélteti.

A rendszer jelenlegi tervében sajnos nem szerepel ilyen elem. De szerencsére az iparágban található erre a problémakörbe megfelelő modul, amit fel lehet használni a probléma kiküszöbölésére. Ez pedig a megfigyelő (watchdog) funkcionalitás, mely monitorozza a WSP[2] működését.

Az IPL-ek hatékonyságát az eléréskori hiba valószínűsége (PFD[3]) határozza meg.

6.2.2. Frekvencia számítás

Az esemény következményének frekvenciáját az alábbi egyenlettel lehet megadni:

$$f^C = f^I \times \prod_{j=1}^{J} PFD_j \tag{6.1}$$

Ahol,

f^C a kimenetel frekvenciája

f^I a kezdeményező esemény frekvenciája és

PDF_j a j-edik IPL hibájának valószínűsége, ami védelmet nyújt a kimenetellel szemben.

[1]Independent Protection Layer

[2]WheelSlide Protection

[3]Probability of Failure on Demand

SIL besorolás	THR[4]	PFD
SIL4	$1e^{-8} < f \leq 1e^{-9}$	$1e^{-3} < f \leq 1e^{-4}$
SIL3	$1e^{-7} < f \leq 1e^{-8}$	$1e^{-2} < f \leq 1e^{-3}$
SIL2	$1e^{-6} < f \leq 1e^{-7}$	$1e^{-1} < f \leq 1e^{-2}$
SIL1	$1e^{-5} < f \leq 1e^{-6}$	$9e^{-1} < f \leq 1e^{-1}$

6.6. táblázat. A SIL besorolások kapcsolata a THRrel és a PFDvel.

Néhányaknak szemetszúhatott már, hogy az IPL-ek esetében On-Demand hiba valószínűségről beszél a szakirodalom, míg a vasútiparban általában folytonos módban vannak megadva a tűrésértékek. Ezért fontos kiemelni, hogy konverzió nélkül nem alkalmazható a fenti egyenlet.

A két szabványrendszer kapcsolatát a 6.6 táblázat írja le. Mivel a rendszer tisztán elektronikus ezért a fejezet elején leírtak szerint a rendszer megbízhatósága $r(t) = e^{-\lambda t}$ közelíthető. Továbbá szitén fentebb említettek szerint a rendszer élettartama 30 év, évi 5000 órás használattal.

Ezért annak a valószínűséget, hogy a rendszer meghibásodik az élettartama során (150 000 óra): $1 - e^{-\lambda * 150000}$ Ezt behelyettesítve a THR-rel megkapható az átlagos PFD értéke.

A forgatókönyhöz tartozó tűrhető kockázat a fenti elemzésekből adodóan $THR > 1e^{-7}$. A csökkentés nélküli frekvencia $1e^{-4}$, tehát a folyamat során legalább három nagyságrenddel kell csökkenteni a lehetséges előfordulást.

Ez úgy érhető el, ha a watchdog funkcióból SIF[5], azaz biztonság-kritikus funkció keletkezik SIL4-es besorolással, hiszen ekkor a fenti egyenlet szerint

$$\mathbf{f}^C = \mathbf{f}^I \times \prod_{j=1}^{J} \mathbf{PDF}_j \tag{6.2}$$

$$= 1e^{-4} \prod 1e^{-3} \tag{6.3}$$

$$= 1e^{-7} \tag{6.4}$$

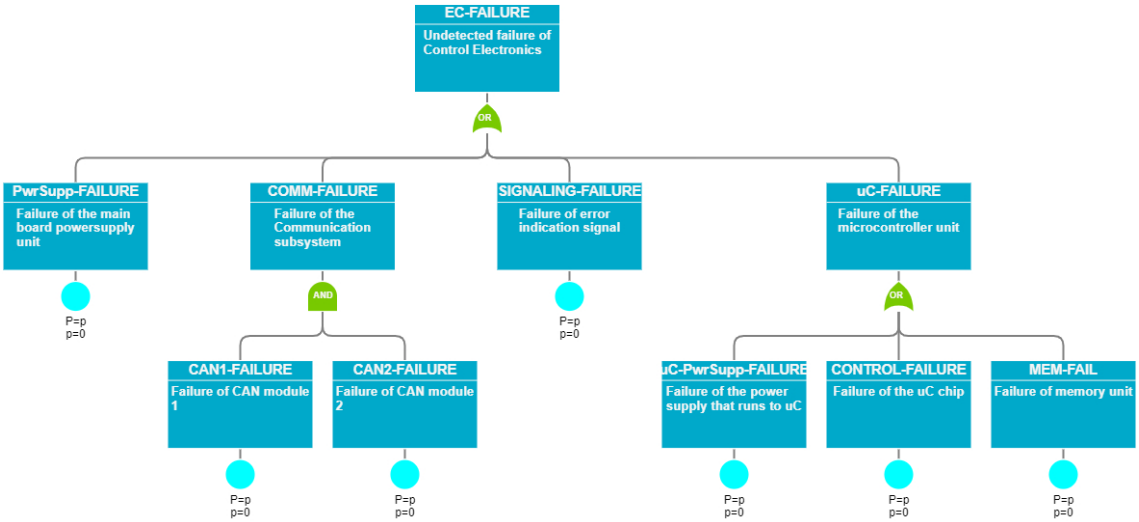
A csökkentett hibaelőfordulás már csak $f > 1e^{-7}$, ami tolerálható.

Ezért a vizsgálat utáni javaslat, hogy a folyamatot fel kell instrumentálni egy hibadetektáló alrendszerrel. Továbbá, mivel egy SIL4-es funkció kifejlesztése nagyon költséges a vállaltra nézve és feltételezve, hogy a SIL2-es funkció ténylegesen képes két nagyságrendű csökkentésre lehetséges még egy modifikációs javaslat. Néhány helyzetben költséghatékonyabb kifejleszteni két SIL2-es funkciót/terméket mint egy SIL4-est. Ezek alapján a másik javaslat, hogy WSP funkcióból is képeznek egy SIF-et, amely így képes csökkenteni saját hibáit ezáltal az alap frekvenciát is. Ha mind a WPS, mind a WPS watchdog részegységek SIL2-es besorolással rendelkeznek az eredő csökkentés $1e^{-4}$, amivel teljesíthető a tűrhető hibaráta követelménye.

6.3. FTA

A hibafa analízis az egyik legalaposabb és legáltalánosabb vizsgálati módszer. Ha van olyan hibakövetkezmény, amit már az előzőleg végrehajtott módszerek felfedeztek, de

[5]Safety Instrumented Function



6.2. ábra. A vezérlőelektronika qualitatív hibafája.

bonyulultsága nem tette lehetővé, hogy részletesebben elemezzék akkor azt általában az FTA vizsgálja ki.

A dolgozatban ez a komplex alegység, melynek vizsgálatát erre a fejezetrészre hagytam, a vezérlő elektronika. Ez az egység csak részben lett megemlítve az előző analízisek során és eddig a pontig csak annyit tudunk róla, hogy a WSP funkció, ami a mikroprocesszoron fut SIL2-es besorolást kapott.

6.3.1. Kvalitatív analízis

Ebben a részben azt a hibát kutatjuk - egyenlőre kvalitatív jellegel -, hogy mekkora valószínűséggel lesz detektálatlan hibamódban a vezérlő elektronika.

A részegység rendelkezik redundáns CAN kommunikációs interfésszel, amelyen képes adatokat fogadni és hibát is jelezni. Az egész alaplap rendelkezik egy táppal, ami a vonat rendszerfeszültségéből képes a többi részegység által szükséges 5V feszültséget konvertálni.

Az alrendszer rendelkezik egy dedikált kommunikációs lehetőséggel, melyen a súlyos hibákat tudja jelezni a vonat szint (Train Level) felé. Elsődlegesen ez a hibajelző rendszer.

Továbbá, a vezérlési funkcióknak helyet adó mikroprocesszor található még az egységben. Ez rendelkezik egy saját dedikált táppal, ami a μC-nek transzformálja a megfelelő feszültségszintet és a programkód számára elérhető memória modullal.

Ez alapján konstruálható olyan hibafa, ami a fent leírtak alapján helyezi el a hibamódokat. Az elkészített hibafa a 6.2. ábrán látható. Ezen látható, hogy nincsen teljesen normál formára hozva, hiszen a felső VAGY kapu alatt található még egy VAGY kapcsolat. Ha teljesen normálalakúra alakítjuk az *uC-FAILURE* kapu alatt lévő elemek egyenesen a Top-event alá kerülnek. Így rendszerben hat darab minimális vágás található.

Item	FR(1/h)	P_failure (150000h)
24V-5V supply	$1.5e^{-7}$	$2.22e^{-2}$
CAN controller	$8e^{-7}$	$1.13e^{-1}$
Signal control	$1.5e^{-7}$	$2.22e^{-2}$
5V-1V2 supply	$1.5e^{-7}$	$2.22e^{-2}$
μC	$1.5e^{-7}$	$2.22e^{-2}$
Memory unit	$1.5e^{-7}$	$2.22e^{-2}$

6.7. táblázat. Feladatban használt hibaráták és hiba valószínűsége

6.3.2. FIT allokáció

A hibafa diagramm rendkívül alkalmas az alegységek logikai sorrendben reprezentálára. Ezt kihasználva elvégezhetjük az EN 50129[2] által csak TFFR[6] elosztását is.

Tegyük fel, hogy már meglévő vizsgálatok alapján és/vagy felsőbb utasítás hatására az a vezérlő elektronika SIL2-es besorolást kapott. Ez azt jelentené, hogy maximum hibaráta amit az egység megengedhez, az $1e^{-6}\frac{1}{h}$. Azt a felvetést követve, hogy a FIT[7] az a 10^9 órán belül történt hibák számát jelöli, a részegység 100 és 1000 FIT közötti értékből gazdálkodhat.

A SIL mellé megkaptuk, hogy a részegységnek 800 FIT-ből kell kigazdálkodni a teljes működését.

Ezt a 800 FIT-et kell elosztani az eggyel alacsonyabb szint felé osztani. Most a már fentebbi fejezeketben említett egyenlő elosztási módszert alkalmazom, így minden alegységre 150 FIT jut, azaz a TFFR 150 FIT.

Mivel a kommunikációs modul két független részből áll, ezért a következő elvetés alkalmazható a további FIT allokációhoz:

$$\mathbf{FFR} \approx 2FR^2 \times SDT \tag{6.5}$$

ahol az SDT a safe down time-ot jelöli.

A képletet használva, 10 órás (nap végi ellenőrzés a detektáció) SDT-vel számolva elegendő lenne 8000 FIT-nek lennie minden egyes CAN csatornának. De mivel ez kritikus funkciót valósít meg, ezért 800 FIT-et allokálok számukra (ami SIL2-es funkcionalitást jelent).

6.3.3. Kvantitatív analízis

A számolások során fiktív értékeket feltételezve a 6.7 táblázatban szereplő értékekkel végzem. Egy projekt során ezek az értékek egy FMECA analíziből származnának.

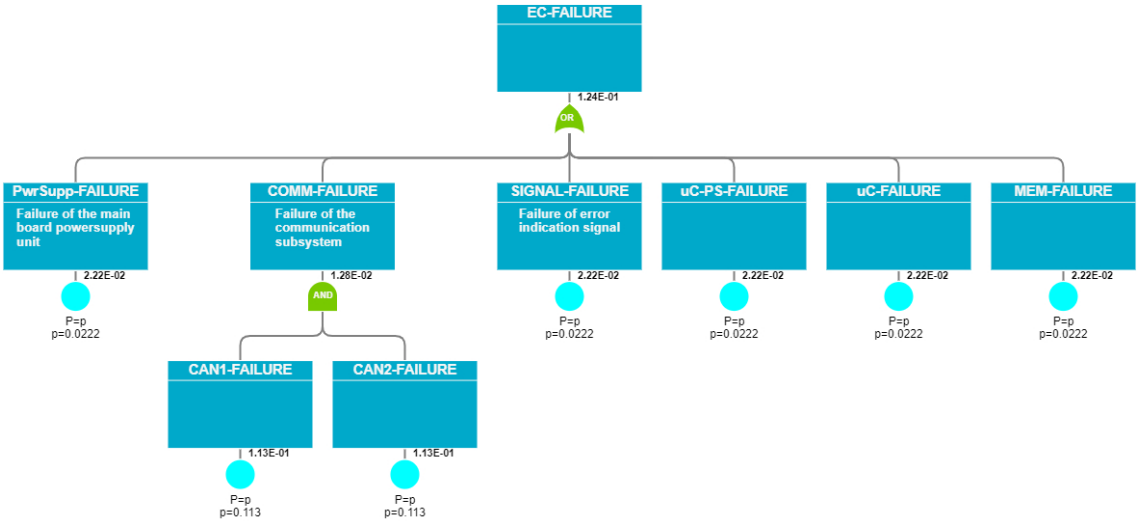
A valószínűségeket az alábbi egyenlet alapján lehet megkapni, a rendszer a fentebb meghatározott élettartama alapján:

$$P = 1 - e^{-\lambda t} \tag{6.6}$$

$$= 1 - e^{-150000\lambda} \tag{6.7}$$

[6]Tolerable Functional Failure Rate

[7]failure in time



6.3. ábra. Kvantitatív FTA az adott értékek alapján

Amint az az 6.3. ábrán látható a kvantitatív analízis elvégzése után látható az alrendszer teljes élelttartamra számított detektálatlan hibájának a valószínűsége. Ez sajnos nem egy szép alacsony szám, de vegyük figyelembe, hogy ez százötven-ezer órára vetített érték és még így is a rendszenszer számára allokált SIL kategóriába tartozik, sőt még a rendszer számára osztott TFFR-en is belül helyezkedik.

7. fejezet

Összefoglalás

A szakdolgozat során felkutattam számtalan a biztonsági analízishez használt módszert. Ezen módszerek nagyrésze már szerepel a vasútipari szabványok valamelyikében, de más iparából is származott hasznos technológia.

A módszerek között megkülönböztettem lehetséges Top-down és Bottom-up irányú eszközöket is, leírva azok előnyét a fejlesztés lépéseinek támogarása során.

A dolgozat során bemutattam a modell-alapú rendszerfejlesztés pár lehetőségét a vasútiparra tekintve. Elkészült a fékrendszer funkcionális modellje/architektúrája. A fejlesztés során bemutattam a funkcionális dekompozíció lépéseit és ezáltal eljutottam egy kinevezett funkció (üzemi fék) alacsonyabb szintjeihez.

A funkcionális dekompozíció Top-down metodikája mellett elkészült a fékrendszer egy platform modellje. Ebben bemutattam a Bottom-up módszertan felépítését, majd a kis komponensekből bemutattam a felépített rendszer modelljét. Ezen a platform architektúrán már megjelentek a fizikai építőelemek és azok összeköttetéseik.

A modellezés végeztével az általam választott módszerekkel biztonsági analízist hajtottam végre az elkészült terveken.

Ebbeb bemutattam a HAZOP, a LOPA és az FTA módszereket. A HAZOP egy magasszintű szisztematikus problémafeltáró eljárás, amely iránymutató szavak segítségével vezetett rá a lehetséges hibákra. A LOPA átmenet a HAZOP és az FTA között. Segítségével egy egyszerű hibát rangsoroltam. Az FTA összetett hibák elemzésére alkalmas eszköz aminek segítségével egy komplex alegység biztonsági vizsgálatát végeztem el.

7.1. Javaslatok további munkára

A jövőben szeretném részletesebben kidolgozni a rendszertervet. Ebbe beletartozik a funkciók részletesebb dekompozíciója és ezen funkciók viselkedésének/kapcsolatainak modellezése. Érdekes lehet még valós adatok/követelmények alapján készíteni a modelleket különböző tervezési kényszer mellett.

Továbbá szeretném tovább részletezni a biztonsági analízist is. Ennél a feladatkörnél is érdekes lehet valós adatok/tények felkutatása és azok alapján végezni a vizsgálatot.

Ábrák jegyzéke

Táblázatok jegyzéke

Irodalomjegyzék

[1] National Aeronautics – Space Administration: Pushing the state of the art: A web-enabled mbse analysis integration framework, phase i. `https://data.nasa.gov/dataset/Pushing-the-State-of-the-Art-A-Web-enabled-MBSE-An/m24q-4s9d`, 2020.

[2] Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling. Standard, London, UK, 2018. mar, The British Standards Institution.

[3] Dependability management — part 1: Dependability management systems. Jelentés, 2003, British Standard.

[4] Dependability management — part 3-1: Application guide — analysis techniques for dependability — guide on methodology. Standard, 2004, British Standard.

[5] Daniel A. Crowl (szerk.): *Layer of Protection Analysis: Simplified Process Risk Assessment (A CPPS Concept Book)*. 2001, American Institute of Chemical Engineers.

[6] Arthur M. Dowell III: Layer of protection analysis and inherently safer processes. *Process Safety Progress*, 18. évf. (1999) 4. sz., 214–220. p. URL `https://aiche.onlinelibrary.wiley.com/doi/abs/10.1002/prs.680180409`.

[7] Railway applications - braking - mass transit brake systems - part 1: Performance requirements. Standard, 2003, CEN.

[8] Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process. Standard, Brussels, BE, 2017. October, CENELEC.

[9] Failure modes and effects analysis. Jelentés, 2006, British Standard.

[10] Sanford Friedenthal – Regina Griego – Mark Sampson: Incose model based systems engineering (mbse) initiative. In *INCOSE 2007 symposium* (konferenciaanyag), 11. köt. 2007.

[11] Clifton A. Ericson II: *Hazard Analysis Techniques for System Safety*. 2005, Wiley-Interscience. ISBN 0471720194,9780471720195.

[12] J.J Kaufmann: Function analysis system technique (fast) for management applications. *Value Word*, 5. évf. (1982).

[13] Zhiqiang Long – Xinwei Wang – Cheng xin Fan: Braking system multi-state analysis of maglev train based on bayesian networks. *2017 Prognostics and System Health Management Conference (PHM-Harbin)*, 2017., 1–8. p.

[14] Military handbook: Electronic reliability design handbook. Jelentés, 1998, US DoD.

[15] Military standard: Procedures for performing a failure mode, effects, and criticality analysis. Jelentés, 1980, US DoD.

[16] OMG: What is sysml. `https://www.omgsysml.org/what-is-sysml.htm`.

[17] Enrico Zio Qamar Mahboob: *Handbook of RAMS in Railway Systems*. 2018, CRC Press.

[18] Railway applications - braking - mass transit brake systems - part 1: Performance requirements. Jelentés, 2013, CENEC.

[19] Reliability block diagrams. Jelentés, 2006, British Standard.

[20] Hong-Seung Roh – Chandra S Lalwani – Mohamed M. Naim: Modelling a port logistics process using the structured analysis and design technique. *International Journal of Logistics Research and Applications*, 10. évf. (2007) 3. sz., 283–302. p. URL `https://doi.org/10.1080/13675560701478240`.

[21] Hendrik Schäbe: *SIL Apportionment and SIL Allocation*. chapter5 fejezet. 2018, CRC Press.
URL `https://www.routledgehandbooks.com/doi/10.1201/b21983-5`.

[22] N. Shevchenko: An introduction to model-based systems engineering (mbse). ="http://insights.sei.cmu.edu/blog/introduction-model-based-systems-engineering-mbse/, 2020.

[23] SysML.org:. `https://sysml.org/`.

[24] SysML.org:. `https://sysml.org/sysml-partners/`.

[25] Molnár Vince: Informatikai rendszertervezés. `https://inf.mit.bme.hu/sites/default/files/materials/category/kateg%C3%B3ria/oktat%C3%A1s/bsc-t%C3%A1rgyak/informatikai-rendszertervez%C3%A9s/20/01-RETE-Overview.pdf`, 2019.

[26] Ronald J. Willey: Layer of protection analysis. *Procedia Engineering*, 84. évf. (2014), 12–22. p. ISSN 1877-7058. 2014 International Symposium on Safety Science and Technology.